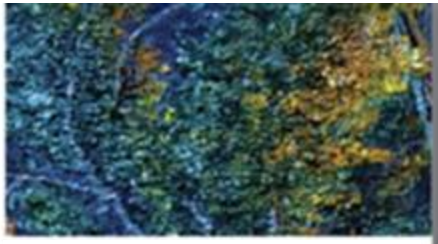


INTERNATIONAL SCIENCE REVIEWS

AIU

№4 (6) 2024

Natural Sciences and Technologies series

www.aiu.kz

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№4 (6) 2024

Astana

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

International Sciense Reviews NST - 76153
International Science Reviews
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

CONTENT

МРНТИ 81.93.29

Құпия ақпаратты алу әдістері мен құралдары

Ш.Қ. Серікова[a]✉, С.А.Наурызбаева[a]

[a]✉ Ақпараттық технологиялар және инженерия жоғары мектебі, Астана халықаралық университеті, 010000, Астана, Қазақстан
Автор-корреспондент

Аңдатпа: Мақалада сандық революцияның ақпараттық қауіпсіздікке тигізген әсері мен оның өзекті мәселелері қарастырылады. Конфиденциалды ақпараттың маңыздылығы артуымен қатар, оның қауіп-қатерге ұшырау ықтималдығы да жоғарылаған. Киберқару және кибершабуылдар заманауи қауіптердің негізгі түрлеріне айналды, ал бұл шабуылдар қаржылық, беделдік және ұлттық қауіпсіздік тұрғысынан айтарлықтай залал келтіруде. Мақалада ақпаратқа рұқсатсыз қол жеткізу әдістері, соның ішінде техникалық арналар мен электромагниттік сәулеленуді пайдалану тәсілдері сипатталып, ақпараттық жүйелерді қорғау бойынша стратегиялық шешімдер ұсынылған.
Кілттік сөздер: ақпараттық қауіпсіздік, киберқауіп, киберқару, құпия ақпарат, техникалық арналар, TEMPEST, электромагниттік сәулелену, ақпараттық жүйелерді қорғау, деректердің қауіпсіздігі.

КІРІСПЕ

Ақпараттық технологиялар дәуірі адамзаттың өмір сүру салтын айтарлықтай өзгертті. Бұл кезең жаңа мүмкіндіктермен қатар, үлкен қауіп-қатерлерді де алып келді. Қазіргі заманда мәліметтер ең маңызды активтердің бірі болып табылады, бірақ олардың құндылығы артқан сайын кибершабуылдар да жиіледі. Мемлекеттік құпиялардан бастап жеке деректерге дейінгі ақпарат шабуыл нысанына айналып, оны қорғау қажеттілігі күшеюде. Мақалада құпия ақпаратты алудың негізгі әдістері, заманауи қауіптердің түрлері және ақпараттық қауіпсіздікті қамтамасыз ету жолдары қарастырылады.

Ақпараттық технологиялар ғасыры адамзатқа жаңа мүмкіндіктер әкелгенімен , сонымен қатар үлкен қауіптерді де тудырды. Сандық революция өмірдің барлық салаларын қамтып, мәліметтерді ең маңызды активтердің біріне айналдырды, бірақ олар сонымен бірге шабуылдардың нысанына айналды. Конфиденциалды ақпарат – мемлекеттік құпиялар, коммерциялық мәліметтер, әскери жоспарлар және жеке деректер сияқты құпия ақпараттың маңыздылығы артқан сайын, олар зиянкестер, жеке хакерлер, киберқарулы топтар да иемденуге тырысады. Сонымен қатар, технологиялардың дамуы деректердің таралу қаупін арттырып, ақпараттық жүйелерді қорғау мәселесін күрделендіре түсті.

Интернет пен ақпараттық технологиялардың дамуымен киберқауіптер қарапайым бұзудан бастап, ауқымды жоспарларға дейін дамыды.

Киберқару – бұл заманауи қауіптердің негізгі түрлерінің бірі, ол тек ақпарат жинау үшін ғана емес, сонымен бірге деректерді жою, маңызды инфрақұрылымдарға кедергі жасау және кибершпионаж жүргізу үшін де қолданылады. Мұндай шабуылдар қаржылық және беделдік тұрғыдан айтарлықтай залал келтіреді, сондай-ақ ұлттық қауіпсіздікке қауіп төндіреді. Екінші жағынан, **киберқауіпсіздік** – бұл деректердің таралуын болдырмауға, ақпараттық дармен байланысты тәуекелдерді азайтуға бағытталған жауапты шаралар жиынтығы. Бүгінгі таңда бұл тек технологиялық мәселе ғана емес, сонымен қатар заңнаманы, ұйымдастырушылық шараларды және деректерді қорғаудың инновациялық тәсілдерін қамтитын стратегиялық бағыт болып табылады.

Cybersecurity Ventures мәліметтері бойынша, киберқылмыстың жаһандық шығыны алдағы үш жылда жылына 15% - ға өседі және 2025 жылға қарай жылына $10,5 трлн-ға жетеді, бұл бір жылдағы табиғи апаттардан көп шығын және барлық негізгі

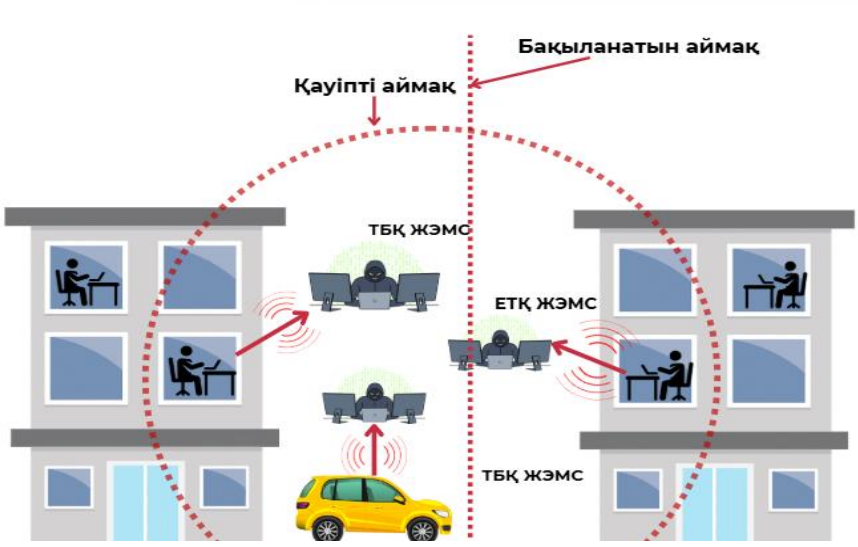
заңсыз есірткілердің жаһандық саудасынан тиімдірек. Киберқылмыс шығындарына деректердің бүлінуі мен жойылуы, ұрланған ақша, өнімділіктің жоғалуы, зияткерлік меншікті ұрлау, жеке және қаржылық деректерді ұрлау, жымқыру, алаяқтық, шабуылдан кейін қалыпты бизнесті бұзу, сот тергеуі, бұзылғандарды қалпына келтіру және жою жатады [1].

Мақалада құпия ақпаратты алу әдістері мен құралдарын, сондай-ақ ақпараттық жүйелерді қорғаудың тәсілдерін қарастырамыз. Мақсат – ақпарат таралуы мен шабуылдардың салдарын барынша азайту үшін тиімді шараларды сипаттау.

Құпия ақпаратқа рұқсатсыз қол жеткізу қазіргі заманғы қауіп-қатерлердің ең өзекті мәселелерінің бірі болып табылады. Ақпаратқа рұқсатсыз қол жеткізудің негізгі тәсілдері техникалық, кибер және психологиялық құралдарды қамтиды. Төменде бұл әдістердің егжей-тегжейлі сипаттамасы мен олардың жұмыс істеу әдістері қарастырылады.

Техникалық каналдар арқылы қол жеткізу. Техникалық каналдар арқылы ақпаратқа қол жеткізу — арнайы құрылғылардың көмегімен ақпаратты тасымалдау немесе өңдеу кезінде пайда болатын сигналдарды ұстап қалу. Бұл әдіс жиі құпия мәліметтерге рұқсатсыз қол жеткізу үшін қолданылады.

Электромагниттік сәулелену. Электрондық құрылғылар жұмыс істегенде электромагниттік сигналдар шығарады. Сигналдарды арнайы қабылдағыштармен ұстап, оларды шифрлау арқылы құпия ақпарат алуға болады. Бұл тәсіл арқылы компьютер мониторындағы бейнелерді немесе пернетақтадағы енгізілген деректерді көреді. Мұндай шабуылдар "TEMPEST" деп аталатын әдістерге жатады.



Сурет 1. Есептеу техникасы құралдарының (ЕТҚ) жанама электромагниттік сәулеленулерін (ЖЭМС) техникалық барлау құралдарымен (ТБҚ) ұстап алу схемасы

Бұл схема есептеу техникасы құралдарының (ЕТҚ) жұмыс барысында пайда болатын жанама электромагниттік сәулеленулерді (ЖЭМС) техникалық барлау құралдарымен (ТБҚ) ұстап алу процесін бейнелейді. Бұл сәулеленулер арнайы құралдармен талданса, өңделіп жатқан деректер туралы ақпаратты қамтуы мүмкін, бұл оларды ақпараттың сыртқа таралуының ықтимал арнасына айналдырады.

Схеманың негізгі элементтері:

Есептеу техникасы құралдары (ЕТҚ) – жанама электромагниттік сәулеленулердің көзі. Бұл деректерді өңдейтін компьютерлер, серверлер немесе басқа да құрылғылар болуы мүмкін.

Жанама электромагниттік сәулеленулер (ЖЭМС) – ЕТҚ жұмысы барысында туындайтын сигналдар. Олар ауа, кабельдер немесе басқа да өткізгіштер арқылы таралады.

Техникалық барлау құралдары (ТБҚ) – жанама сәулеленулерді анықтауға, қабылдауға және талдауға арналған құрылғылар. Олар мыналарды қамтуы мүмкін:

Схеманың мақсаты: Схема ТБҚ-дың физикалық ортада таралатын жанама сәулеленулерді қалай ұстап, олардың ішінен құпия ақпаратты қалай алатынын көрсетеді [2].

Компаниялар мен мемлекеттік мекемелер мұндай ақпараттың сыртқа таралуын болдырмау үшін жабдықты экрандау, қорғалған аймақтар құру сияқты арнайы шараларды қолданады.

Дыбыс толқындары арқылы тыңдау. Сөйлесу немесе басқа да дыбыстар микрофондар немесе бөлмедегі дыбыстарды ұстап қалуға арналған лазерлік құрылғылар арқылы қабылданады. Бұл әдіс, әсіресе, кеңселердегі жабық келіссөздер немесе құпия жиналыстар кезінде жиі пайдаланылады.

Оптикалық әдістер. Жасырын камералар немесе инфрақызыл сканерлер арқылы кеңседегі құжаттарды, экрандарды немесе әрекеттерді бақылау әдісі. Кейбір жағдайларда лазерлік сәулелену терезе әйнегіне бағытталып, бөлмедегі дыбыстарды тіркеуге мүмкіндік береді.

Провайдерлік желілерді тыңдау. Мәліметтерді беру кезінде интернет немесе телефон желілеріндегі сигналдарды ұстап қалу арқылы ақпаратқа қол жеткізіледі. Бұл әдіс әсіресе интернет немесе телекоммуникация жүйелері арқылы ақпарат жіберу кезінде жиі қолданылады.

Арнайы зиянды бағдарламалар ақпараттық жүйелердің ең әлсіз тұстарын пайдалана отырып, ақпаратқа қол жеткізуге мүмкіндік береді.

Фишинг —Қолданушыларды алдап, құпия ақпаратты (логиндер, құпиясөздер) алуға бағытталған әдіс. Фишинг шабуылдары электрондық хаттар, жалған веб-сайттар немесе мессенджерлер арқылы жүзеге асады. Мысалы, жалған хаттар арқылы қолданушыдан құпиясөзін енгізуді талап етеді.

Мәліметтерді ұрлайтын зиянды программаларға трояндар, кейлоггерлер және шпиондық программалар жатады.

Кейлоггерлер: Пернетақтада терілген мәтіндерді тіркеп, деректерді зиянкестерге жіберетін құралдар. Яғни компьютер пайдаланушыларының пернетақтадағы пернелерді басуын тіркеу. Шпиондық бағдарламалық жасақтаманың бұл түрі аппараттық және бағдарламалық әдістер арқылы жұмыс істей алады, енгізілген ақпаратты тіркейді және оны шабуылдаушыларға жібереді. Бағдарламалық жасақтама кілттері ең көп таралған және компьютерлерге немесе мобильді құрылғыларға пайдаланушы байқамай орнатылады. Олар барлық пернелерді басу арқылы фондық режимде жұмыс істейді. Аппараттық пернетақта тыңшылары-бұл компьютерге қосылатын физикалық құрылғылар. Олар әдетте пернетақта мен компьютер арасында орнатылады [3].

Трояндар: Жүйеге заңсыз кіріп, құпия ақпаратты тасымалдауға арналған зиянды кодтар. Жүйеге және файлдарға әсер ететін компьютерлік вирустың ерекше түрі; деректерді уақытында бүлдіруі мүмкін және басқа компьютерлерге, құрылғыларға және смартфондарға USB құрылғысын

жұқтырып, ұқсас деректерді беру құрылғылары арқылы таратуға тырысады. Трояндық бағдарламаның көпшілігі конфиденциалды ақпараттарды жинау үшін арналған. Мұндай мәліметтерге қолданушы парольдері жатады, бағдарламаның тіркеу нөмірлері, банктік шот туралы мәліметтер және т.б. Басқа трояндықтар компьютерлік жүйеге зиян ету үшін құрылады, оларды жұмыс істей алмайтын жағдайға жеткізеді [4].

Шпиондық программалар: Құрылғыдағы әрекеттерді бақылау және мәліметтерді сыртқа шығару үшін қолданылады.

Ең жиі қолданылатын DdoS-шабуылы. DDoS шабуылы (Distributed Denial of service – қызмет көрсетуден бас тарту) – көптеген жалған сұраныстар беру арқылы ақпараттық инфрақұрылымға хакерлік шабуыл. DDoS-ең көп таралған және қауіпті шабуылдардың бірі, көбінесе бопсалау, қорқытып алу, деректерді ұрлау, ақпараттық соғыс мақсатында жасалады. Интернеттің жарты сағат ішінде болмауы (тіпті бірнеше күн) жұмыстың тоқтап қалуына, бизнес-процестердің бұзылуына, қаржылық шығындарға, ақпараттың жоғалуына және клиенттердің наразылығына қауіп төндіреді [5].

Мәліметтерді шифрлау. Зиянкестер мәліметтерді шифрлап, оларды тек төлем жасалған жағдайда қайтаруға уәде береді. Бұл шабуылдар "Ransomware" деп аталады.

Әлеуметтік инженерия — адамның психологиялық осал тұстарын пайдаланып, оған рұқсатсыз немесе қасақана әрекеттер жасауға итермелеу арқылы құпия ақпарат алудың әдісі. Бұл тәсілдер көбінесе адамның сеніміне кіріп, ұйымдардың ішкі процестеріне кіру үшін қолданылады. Әлеуметтік инженерия әдістерінің негізгі түрлері мен олардың жұмыс істеу принциптері.

Құпиясөздерді ұрлау: Қызметкерлердің әлсіз немесе қарапайым құпиясөздерін алу үшін, фишингтің элементтері арқылы жасырын шабуылдар жасалады.

Клондау (Spoofing): Құрылғы немесе жүйе құпия ақпаратты ұрлау мақсатында басқа құрылғы немесе жүйе ретінде көрсетіледі. Бұл жағдайда құрылғының немесе сервердің сәйкестігі жасалып, дұрыс ақпарат беріледі[6].

Жалған қызметкерлер (Impersonation): Құрылымдарда басқа адамның немесе компанияның қызметкері ретінде танысып, олардың қауіпсіздік шараларын бұза отырып, ақпарат алуға тырысу.

USB арқылы құпия ақпарат алу: Тегін бағдарламалық қамтамасыз ету немесе мәліметтерді көшіру үшін "тегін" USB құрылғылары беріледі. Бірақ бұл құрылғыларда зиянды бағдарламалар болуы мүмкін, олар құрылғыға қосылған кезде мәліметтерді ұрлайды.

Жалған телефон қоңыраулары: Құрбандарға заңды ұйымнан немесе мемлекеттік қызметкерден телефон қоңырауы келіп, олардың жеке мәліметтерін немесе банктік ақпараттарын сұрайды. Тіпті қәзір

Әлеуметтік инженерия әдістері адамдардың психологиялық осал тұстарын пайдалану арқылы құпия ақпарат алуды мақсат етеді. Бұл әдістердің тиімділігі олардың адамның сеніміне кіру және оны өз еркімен ақпарат беруге итермелеуіне негізделген. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету үшін тек техникалық шаралар ғана емес, сонымен қатар қызметкерлердің және ұйымдардың ақпараттық қауіпсіздікке қатысты сауаттылығын арттыру қажет.

Интернеттегі ашық ақпаратты жинау. OSINT (Open Source Intelligence) ашық көздерден ақпарат жинау әдісі, ол ақпаратты құпиялылықты бұзбай және заңды түрде алу принципіне негізделеді. OSINT ақпаратты жинаудың ең танымал және тиімді әдістерінің бірі болып табылады. Бұл ақпаратты мемлекеттік органдар, заңнамалық органдар, қауіпсіздік қызметтері, журналистер, зерттеушілер, сондай-ақ киберқылмыскерлер, ұйымдар мен компаниялар да пайдаланады[7]. OSINT-тің негізгі көздері: Әлеуметтік желілер (Facebook, Twitter, Instagram, LinkedIn, TikTok, және басқалар) OSINT жинау үшін маңызды ақпарат көздері болып табылады.

Тікелей қол жеткізе алмайтын мәліметтерді алу үшін зиянкестер объектілерге қосымша құрылғылар орнатады.

- **GPS трекерлер:** Қозғалыс траекторияларын қадағалау үшін.
- **Жасырын микрофондар мен камералар:** Кеңседегі сөйлесулер мен іс-әрекеттерді тіркеу үшін орнатылады.
- **Wi-Fi тыңдау құрылғылары:** Желілік трафикті ұстап қалу және ақпаратты шифрын ашу үшін қолданылады.

Құпия ақпартты алу барысында техникалық құралдар мен құрылғылардың рөлі өте маңызды, әсіресе сигнал генераторлары, цифрлық зондтар ақпаратты алудың тиімді әдістері болып табылады. Бұл құралдар ақпаратты жиналуына, оның бөлініп кетуіне, және қорғалуына байланысты әртүрлі процестерді бақылауға мүмкіндік береді.

Сурет 2. Сигнал генераторлары

Сигнал генераторлары — электрондық құрылғылар, олар белгілі бір жиіліктегі электромагниттік сигналдар шығарады. Бұл сигналдар заңсыз құрылғыларды бақылау үшін қолданылуы мүмкін. Әртүрлі құралдар мен датчиктер арасындағы байланыстар мен сигналдарды бақылай отырып, белгілі бір ақпаратты алу үшін қолданылады.

Цифрлық зондтар — бұл ақпарат алу мақсатында қолданылатын техникалық құралдар. Олар компьютер және басқа техникалық жүйелердің электрондық құрылғыларымен байланысып, деректерді жинайды. Интернет арқылы немесе жергілікті желі арқылы өтетін ақпаратты бақылап, қадағалауға мүмкіндік береді[9].

Ақпаратты қорғау үшін заманауи бақылау әдістері мен құралдары

қолданады. Оларға мыналар жатады:

Деректерді шифрлау. Шифрланған деректер ағып кеткен жағдайда зиянкестер үшін қол жетімді емес.

Деректерді бақылау және талдау.

Қызметкерлерді оқыту. Семинарлар мен тренингтер арқылы қызметкерлердің киберқауіпсіздік туралы хабардарлығын арттыру фишинг пен әлеуметтік инженерияның басқа түрлерінің алдын алуға көмектеседі.

Бағдарламалық жасақтаманы үнемі жаңартып отыру. Бағдарламалық жасақтаманы үнемі жаңартып отыру және патчтарды орнату осалдықтарды жояды.

Жүйелерді үнемі бақылау және ақпараттық ағып кетуді алдын ала анықтау.

Құрылғылардың қауіпсіздік параметрлерін үнемі тексеру[10].

Құпия ақпаратты алу әдістері мен құралдары заманауи технологиялардың дамуымен күрделеніп, түрленіп отырады.

Бұл ақпараттық қауіпсіздік мәселелерін күшейту керектігін білдіреді. Тиімді қорғау үшін ұйымдар кешенді тәсілдер мен заманауи шешімдерді қолдануы қажет. Тек осындай шаралар арқылы ақпараттық ресурстардың құпиялығы мен тұтастығын қамтамасыз етуге болады.

Қорытынды

Ақпараттық қауіпсіздік – қазіргі заманның ең өзекті мәселелерінің бірі. Техникалық құралдардың күрделенуі және кибершабуылдардың көбеюі деректерді қорғаудың маңыздылығын арттырды. Тек технологиялық шешімдер ғана емес, заңнамалық, ұйымдастырушылық және психологиялық шаралар кешенін қолдану арқылы ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуге болады. Жаңа қауіп-қатерлерге қарсы тиімді стратегия құру – ұйымдар мен мемлекеттердің алдында тұрған негізгі міндеттердің бірі.

Әдебиеттер

[1] https://allinsurance.kz/articles/analytical/20057-top-20-prognozov-pokiberprestupnosti-na-2023-god;
[2] А. И. Белоус & В. А. Солодуха Кибероружие и кибербезопасность. О сложных вещах простыми словами – Инфра-Инженерия, 2020.
[3] https://translated.turbopages.org/proxy_u/ru-kk.ru.179cf6d9-675042ec-3a10ae1a-74722d776562/https/ru.wikipedia.org/wiki/Кейлогер
[4] https://ru.wikipedia.org/wiki/Троянская_программа
[5]]https://translated.turbopages.org/proxy_u/ru-kk.ru.651a9558-6750437e-711f0b30-74722d776562/https/ru.wikipedia.org/wiki/DoS-атака
[6] Гуржиева, Л. И. Информационная безопасность: Учебное пособие. Москва: Юрайт, 2021.
[7] Солдаткин, В. И. Теория и практика информационной безопасности. Санкт-Петербург: Питер, 2020.
[8] Снегур, А. В. Основы защиты информации: Учебное пособие. Москва: Академия, 2019.
[9] Кашкаров, А. П. Информационная безопасность: Защита персональных данных. Москва: ДМК Пресс, 2022.
[10] Белов А. С. Модернизация системы информационной безопасности = Modernization of the Information Security System: The Approach to Determining the Frequency: подход к определению периодичности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. - 2022. - № 4. - С. 76-80.

References

[1] https://allinsurance.kz/articles/analytical/20057-top-20-prognozov-pokiberprestupnosti-na-2023-god;
[2] A. I. Belous & V. A. Solodukha Cyber Weapons and Cybersecurity. About complex things in simple words – Infra-Engineering, 2020.
[3] https://translated.turbopages.org/proxy_u/ru-kk.ru.179cf6d9-675042ec-3a10ae1a-74722d776562/https/ru.wikipedia.org/wiki/Кейлогер
[4] https://ru.wikipedia.org/wiki/Троянская_программа
[5] https://translated.turbopages.org/proxy_u/ru-kk.ru.651a9558-6750437e-711f0b30-74722d776562/https/ru.wikipedia.org/wiki/DoS-атака
[6] Gurzhieva, L. I. Informatsionnaya bezopasnost': Uchebnoe posobie [Information Security: A Textbook]. Moscow: Yurayt, 2021.
[7] Soldatkin, V. I. Teoriya i praktika informatsionnoy bezopasnosti [Theory and practice of information security]. St. Petersburg: Piter, 2020.
[8] Snegur, A. V. Osnovy zashchita informatsii: Uchebnoe posobie [Fundamentals of information protection: Textbook]. Moscow: Academy, 2019.
[9] Kashkarov, A. P. Informatsionnaya bezopasnost': Zashchita personal'nykh dannykh [Information security: Protection of personal data]. Moscow: DMK Press, 2022.

[10] Belov A. S., Dobryshin M. M., Shugurov D. E. Modernization of the Information Security System = Modernization of the Information Security System: The Approach to Determining the Frequency: An Approach to Determining the Periodicity / A. S. Belov, M. M. Dobryshin, D. E. Shugurov // Information Protection. Inside. - 2022. - № 4. - P. 76-80.

Методы и средства получения конфеденциальной информации

Шапагат Серикова [a], Сая Наурызбаева [a]

[a] Высшая школа информационных технологий и инженерии, Международный университет Астана, 010000, Астана, Казахстан

Аннотация. В статье рассматриваются влияние цифровой революции на информационную безопасность и ее актуальные проблемы. Наряду с возрастанием важности конфиденциальной информации, возросла и вероятность того, что она подвергнется риску. Кибероружие и кибератаки стали основными видами современных угроз, и эти атаки наносят значительный ущерб с точки зрения финансовой, репутационной и национальной безопасности. В статье описаны методы несанкционированного доступа к информации, в том числе способы использования технических каналов и электромагнитного излучения, предложены стратегические решения по защите информационных систем.
Ключевые слова: информационная безопасность, кибербезопасность, кибероружие, конфиденциальная информация, технические каналы, TEMPEST, электромагнитное излучение, защита информационных систем, безопасность данных

Methods and means of obtaining confidential information

Shapagat Serikova[a], Saya Nauryzbayeva[a]

[a] Higher School of Information Technology and Engineering, Astana International University, 010000, Astana, Kazakhstan

Abstract. The article examines the impact of the digital revolution on information security and its current problems. Along with the increasing importance of confidential information, the likelihood that it will be at risk has also increased. Cyber weapons and cyber attacks have become the main types of modern threats, and these attacks cause significant damage in terms of financial, reputational, and national security. The article describes methods of unauthorized access to information, including ways to use technical channels and electromagnetic radiation, and suggests strategic solutions to protect information systems.
Keywords: information security, cybersecurity, cyberweapons, confidential information, technical channels, TEMPEST, electromagnetic radiation, information system protection, data security.